**Ubutu OpenVPN 2.4.x**

**sudo 권한 부여**

$ sudo visudo //etc/sudoers.tmp 수정

# User privilege specification

사용자 ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command

%sudo ALL=(ALL:ALL) ALL

사용자 ALL=(ALL:ALL) ALL //<- sdn에 sudo 권한 부여

Ctrl+x -> /etc/sudoer.tmp 에서 확장자 제외한 /etc/sudoer로 저장

$ su 사용자 //sdn으로 전환

**//CA Server & OpenVPN Server 같은 HOST에 구성으로 테스트 구축**

$ sudo apt install easy-rsa

$ make-cadir /home/사용자/openvpn //인증키 발급 디렉토리 생성

~/openvpn : easyrsa openssl-easyrsa.cnf **vars** x509-types

인증 관련 키발급 기본 설정 파일 vars 수정, 인증서 키 정보 키 추가

$ vi vars

텍스트이(가) 표시된 사진

자동 생성된 설명

**인증키 생성**

**CA 초기화 (증명서 생성 환경 생성)**

$ ./easyrsa init-pki

init-pki complete; you may now create a CA or requests.

Your newly created PKI dir is: /root/EasyRSA-3.0.0-rc1/pki

**인증기관(CA) 증명서 생성**

$ ./easyrsa build-ca //(nopass 비밀번호 패스 설정)

Common name(참조 인증기관)은 default Easy-RSA CA로 사용하려면 그냥 Enter

CA 증명서, DH키 : ./pki/.

Server/client 증명서 : ./pki/issued/.

개인키: ./pki/private/.

$ ll pki //ca.crt 인증서 (공개키 정보 포함)

$ ll pki/private //ca.key 인증키 (CA 서버에서 사용하는 개인키)

$ sudo cp pki/ca.crt /etc/openvpn/server/

**OpenVPN 서버 증명서와 개인키 생성**

$ ./easyrsa build-server-full server nopass

Enter pass phrase … ca.key: -> CA 증명서 만들 때 입력한 비밀번호 입력 (CA 증명서와 키로 서명)

$ ll pki/issued/server.crt //OpenVPN server 공개키에 해당

$ ll pki/private/server.key //서버 개인키, keypair 파일

$ ll pki/reqs/server.req //인증 요청 파일

RSA 방식으로 송신자/수신자 통신 할 때, 메시지 수신자에 해당하는 OpenVPN Client 는

CA 서버에서 개인키를 발급받아야 메시지 확인할 수 있다

server.key는 OpenVPN server가 Client와 통신하기 위해 필요한 개인키

server.csr

Certificate Signing Request(인증서 서명 요청) : 인증서 발급을 위한 필요 정보를 담고 있는 인증서 신청 형식 데이터, CSR 내용에는 공개키와 인증서가 적용되는 도메인 정보, OpenVPN 서버 설정에 사용

sudo cp pki/issued/server.crt /etc/openvpn/server/

sudo cp pki/private/server.key /etc/openvpn/server/

**Diffie-Hellman(DH) 키 생성 (vars set\_var EASYRSA\_ALGO 옵션이 ec이면 생략)**

$ ./easyrsa gen-dh

$ sudo cp pki/dh.pem /etc/openvpn/server/

**Hash-based Message Authentication Code (HMAC) 키 생성**

OpenVPN 2.4.x

$ sudo openvpn --genkey --secret ta.key //openvpn –genkey –secret /etc/openvpn/server/ta.key

$ sudo cp ta.key /etc/openvpn/server/

OpenVPN 2.5.x : openvpn –genky tls-auth ta.key

SSL/TLS Handshake 패킷에 HMAC 서명을 추가, HMAC서명이 없으면 UDP 패킷을 거부할 수 있다.

포트스캔, OpenVPN UDP port에 대한 DOS 공격,

권한 없는 기기의 SSL/TLS Handshake, SSL/TLS 버퍼 오버 플로우 취약성에 대한 공격 방지함

//생성 files

pki/ca.crt

pki/private/ca.key

pki/reqs/server.req

pki/private/server.key

pki/issued/server.crt

pki/dh.pem

ta.key

|  |  |  |
| --- | --- | --- |
| **인증서/인증키** | **대상** | **목적** |
| ca.crt | 서버와 클라이언트 | 루트 CA 서버 인증서 |
| ca.key | CA 서버 Only | 루트 CA 서버 인증키 |
| server.key | Server Only | Server 개인키 |
| server.crt | Server Only | Server 인증서 |
| dh.pem | Server Only | Diffie Hellman Parameter |
| client1.crt | Client1 Only | Client1 인증서 |
| client1.key | Client1 Only | Client1 개인키 |
| client2.crt | Client2 Only | Client2 인증서 |
| client2.key | Client2 Only | Client2 개인키 |

**Client 증명서/개인키 생성 (client 마다)**

$ ./easyrsa build-client-full ‘사용자증명서명’ nopass

ll pki/issued/client1.crt ll pki/private/client1.key ll pki/reqs/client1.req

// .. 아래 증명서만 만들어도 확인 가능

$ ./easyrsa gen-crl

-> CA 인명서 비밀번호 입력

$ sudo cp pki/crl.pem /etc/openvpn/crl.pem

$ sudo chmod o+r /etc/openvpn/crl.pem

//클라이언트 인증서 모아서 관리

mkdir -p ~/client-configs/keys

chmod -R 700 ~/client-configs

cp pki/private/client1.key ~/client-configs/keys/

cp pki/issued/client1.crt ~/client-configs/keys/

서버인증서와 ta.key 클라이언트 인증서 모아둔 DIR에 복사

cp /pki/ca.crt ~/client-configs/keys/

cp ta.key ~/client-configs/keys/

/\*

<https://jimnong.tistory.com/1367>

\*/

**OpenVPN Server 설정**

$ ll /usr/share/doc/openvpn/examples/sample-config-files //sample copy

$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/server/

$ sudo gzip -d /etc/openvpn/server/server.conf.gz //unzip

//sudo gunzip /etc/openvpn/server/server.conf.gz

$ sudo systemctl status openvpn.service //start, stop

$ sudo nano **/etc/openvpn/server/server.conf**

ca ca.crt // /etc/openvpn/server/ca.crt 패스 지정도 가능

cert server.crt

key server.key

dh dh.pem

crl-verify crl.pem // ./easyrsa gen-crl 로 생성한 client 증명서

tls-auth ta.key **0** //HMAC 키, 모바일 호환 문제가 있기 때문에 사용하는 경우 key-direction 은 ‘**0**’ 지정

key-direction 0

dev tun //tun~ 가상 인터페이스를 생성하여, VPN 가상 네트워크 구성 (모바일 이 방식만 가능)

OpenVPN 데몬(서비스) 권한 축소 실행, 외부 공격 방지위해 주석 처리 권장

(개발 시는 사용이 편함)

cut -f1 -d: /etc/passwd //user목록에 nobody 여부 확인

cut -f1 -d: /etc/group //group목록에 nobody 여부 확인

-> ex: user에 nobody, group에 nogroup이(nobody없음) 있으면 user nobody유지, group nogroup

user nobody

group nogroup

port 1194 //443

proto udp //tcp

explicit-exit-notify 0 // 서버 재시작 알림, UDP 프로토콜이면 기본값 1, TCP는 0

//클라이언트 가상IP 주소 저장, OpenVPN 중단/재시작 되면 ipp.txt 읽어서 동일 가상IP 주소 할당

ifconfig-pool-persist /var/log/openvpn/ipp.txt

VPN 내부 IP 대역(VPN subnet) 설정, VPN 터널링 가상 디바이스 tun에 할당 되는 가상 IP 대역

VPN 내부 IP대역은 10.8.0.0/24로 구성, OpenVPN 서버 내부 IP는 10.8.0.1로 할당

**server 10.8.0.0 255.255.255.0**

텍스트이(가) 표시된 사진

자동 생성된 설명

VPN 접속한 Client의 모든 트래픽은 VPN Server를 경유하게 설정

push “redirect-gateway def1 bypass- dhcp”

특정 DNS 서버 지정 옵션, 내부 DNS서버가 있으면 내부 DNS서버로 변경

push “dhcp-option DNS 8.8.8.8”

다른 내부 IP로 변경 (공유기 상단에 OpenVPN서버를 두면 push “route 192.168.0.0 255.255.255.0”, 공유기에 맞게 변경, 192.168.x.0)

push “route 192.168.10.0 255.255.255.0”

push “redirect-gateway def1 bypass- dhcp”

push “route 10.8.0.0 255.255.255.0” //VPN에서 사용하는 private ip와 subnet마스크를 client에 전달

push “dhcp-option DNS 8.8.8.8”

압축

;compress lz4-v2 //2.4.x 보다 아래 버전인 경우 클라이언트 호환문제 발생, comp-lzo만 사용

;push “compress lz4-v2”

comp-lzo //lzo 패키지를 통해 VPN 접속 시 패킷 압축 옵션

;max-clients 100

//유지(persist)된 데이터에 접근 option

persit-key //재시작 후에도 키 값 유지 (재시작시 접근 권한 없는 리소스 접근 금지 옵션)

persist-tun //재시작 후에도 가상 디바이스 tun 유지

;client-to-client //Client들 끼리 OpenVPN Server를 통해 VPN 터널링 통신

**-> 홈서버 + 공유기 테스트 환경은 client-to-clinet, redirect-gateway def1 필수 사용해야**

**홈서버 내부IP(192.168.x.y)로 접근 가능하고 외부IP주소는 OpenVPN 서버 외부IP로 할당됨**

keepalive 10 120 //10초 주기 ping, 120초동안 수신 없으면 연결 끊어진 것으로 판단

https://community.openvpn.net/openvpn/wiki/CipherNegotiation#Serverversion2.5Configuring:--data-ciphers

패킷 암호 방식 OpenVPN 2.4.x

**cipher AES-256-CBC** //2.5.x에서 사용하려면 data-ciphers-fallback AES-256-CBC

OpenVPN 2.5.x 패킷 암호화 방식 변경

**cipher AEC-256-GCM**

auth SHA256

status /var/log/openvpn-status.log //현재 상태 로그 파일

//Use one or the other(but not both)

log /var/log/openvpn.log //syslog 대신 openvpn log 사용, openvpn 시작 시, truncate(갱신)

log-append /var/log/openvpn.log //openvpn 시작 시 추가

로그옵션 미사용 : grep VPN /var/log/syslog, 사용 : cat /var/log/openvpn.log

;mute 20 //연속 반복 출력되는 메시지 최대 개수 까지만 로그파일에 기록

;duplicate-cn //클라이언트들을 하나의 키로 인증 옵션

;learn-address ./script // 클라이언트 그룹별 방화벽 정책 다르게 지정할 수 있는 옵션

//별도 지정 가능

tls-version-min 1.2

tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-256-CBC-SHA:TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA:TLS-DHE-RSA-WITH-AES-128-CBC-SHA:TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA

verb 4 // Log level, 0, 3, 4(적정), 5~6 접속에러 디버그, 9

------------------------------------------------------------------------------

sudo openvpn –config /etc/openvpn/server/server.conf

//Background 실행

**sudo openvpn –config /etc/openvpn/server/server.conf --daemon**

//홈네트워크 TEST 환경

**IP forwarding 설정 : VPN 접속해서 인터넷에 연결하기 위한 설정**

$ sudo nano /etc/sysctl.conf

# Uncomment the next line to enable packet forwarding for IPv4

net.ipv4.ip\_forward=1 로 변경

net.ipv6.conf.all.forwarding=1 //ipv6

$ sudo sysctl -p //변경 적용

현재 네트워크 인터페이스 확인

ip route | grep default

방확벽 설정

$ sudo ufw status